Algebraic Cayley Differential Space–Time Codes

Frédérique Oggier and Babak Hassibi

***Abstract*—Cayley space–time codes have been proposed as a solution for coding over noncoherent differential multiple-input multiple-output (MIMO) channels. Based on the Cayley transform that maps the space of Hermitian matrices to the manifold of unitary matrices, Cayley codes are particularly suitable for high data rate, since they have an easy encoding and can be decoded using a sphere-decoder algorithm. However, at high rate, the problem of evaluating if a Cayley code is fully diverse may become intractable, and previous work has focused instead on maximizing a mutual information criterion. The drawback of this approach is that it requires heavy optimization which depends on the number of antennas and rate. In this work, we study Cayley codes in the context of division algebras, an algebraic tool that allows to get fully diverse codes. We present an algebraic construction of fully diverse Cayley codes, and show that this approach naturally yields, without further optimization, codes that perform similarly or closely to previous unitary differential codes, including previous Cayley codes, and codes built from Lie groups.**

***Index Terms*—Cayley codes, differential unitary modulation, division algebras, full diversity.**

I. Introduction

It is now well known that multiple antennas at the transmitter and receiver ends of a wireless system help increasing the data rate. Both the scenarios where the receiver knows the channel (*coherent case*) or alternatively does not know the channel (*noncoherent case*) have been largely studied. In particular, design of space–time codes to exploit the diversity of wireless systems have attracted a lot of attention. For the noncoherent multiple-input multiple-output (MIMO) channel, a popular strategy is to use unitary differential modulation [4], [5], which requires the design of unitary matrices that are *fully diverse*, that is, that satisfy the condition that the difference of any two distinct matrices is full rank.

There has been a lot of work on differential space–time coding. In [8], a systematic parameterization for the two antenna case has been done. Among the algebraic approaches, in [16], representation of fixed-point free groups has been considered, while in [6], [7], representation of Lie groups has been investigated. The drawback of all these approaches is that it is difficult to use them to get high-rate codes. In [3], Cayley codes have been introduced to construct differential codes for high data rate. The idea is to use the Cayley transform that maps the space of Hermitian matrices to the manifold of unitary matrices, which yields an easy encoding, and makes Cayley codes available at high rate. Furthermore, they can be decoded using a modified sphere-decoder algorithm [2], [18]. However, the full diversity criterion is difficult to handle, and instead, the authors of [3] suggest another design criterion, based on mutual information. The drawback of Cayley codes is that optimizing the mutual information criterion requires heavy numerical computations, and depends on the number of antennas and rate.

At the same time, *division algebras* have been introduced for coding over coherent MIMO channels [15], [11]. These algebraic objects became of interest, since they naturally provide families of fully diverse matrices. Division algebras have already been investigated in the context of differential space–time coding in [10], [12], where a technique to find unitary matrices inside the fully diverse family of matrices provided by the algebra is described.

The idea of this work is to combine those two approaches: to use division algebras to construct fully diverse Hermitian matrices, and then to apply the Cayley transform to generate fully diverse unitary Cayley codes. This technique yields Cayley codes in closed-form expression, i.e., the encoding matrices are explicitly available from the algebra structure. We are interested in the performance of fully diverse Cayley codes compared to previous differential schemes, in particular to mutual information optimized Cayley codes. Note that we will not try to optimize the proposed Cayley codes on purpose, in order to avoid the known Cayley codes drawback. We thus clearly do not expect the new codes to perform systematically better than each individual code optimized for a given dimension or rate, but we will show that the new approach yields Cayley codes that naturally behave, for different number of transmit antennas, similarly or closely to previous differential codes: previous Cayley codes for two, three, or four transmit antennas, Lie groups based codes for three and four transmit antennas. This fulfills the challenge of getting a family of codes that simultaneously work well or nearly as well, in several dimensions, than previous codes optimized for a given dimension.

The rest of the correspondence is organized as follows: we recall first unitary differential modulation and the construction of Cayley codes in Section II. We then introduce division algebras in Section III, where we explain how to use them to build fully diverse Hermitian matrices. Section IV contains the code constructions together with their simulations.

II. Cayley Differential Codes

We start by briefly recalling the idea behind unitary space–time modulation, before introducing Cayley codes.

A. Differential Unitary Space–Time Modulation

Consider a Rayleigh flat-fading channel with M transmit antennas and N receive antennas, with *unknown channel information*. The channel is used in blocks of M channel uses, so that the transmitted signal can be represented as an $M \times M$ matrix $\boldsymbol{S}_t$, where $t = 0, 1, \ldots,$ represents the block channel use. If we assume that the channel is constant over M channel uses, we may write it as

$$\boldsymbol{Y}_t = \sqrt{\rho}\boldsymbol{S}_t\boldsymbol{H}_t + \boldsymbol{W}_t, \qquad t = 0, 1, \ldots . \tag{1}$$

Here $\boldsymbol{H}_t$, the channel matrix, and $\boldsymbol{W}_t$, the noise matrix, are two $M \times N$ matrices with independent complex normal coefficients, and ρ is the expected signal-to-noise ratio (SNR) at each receive antenna.

We use *differential unitary space–time modulation* [4], [5]. The transmitted signal $\boldsymbol{S}_t$ is encoded using differential modulation, that is (assuming $\boldsymbol{S}_0 = \boldsymbol{I}$)

$$\boldsymbol{S}_t = \boldsymbol{V}_{z_t}\boldsymbol{S}_{t-1}, \qquad t = 1, 2, \ldots \tag{2}$$

where $z_t \in \{0, \ldots, L-1\}$ is the data to be transmitted, and $\mathcal{C} = \{\boldsymbol{V}_0, \ldots, \boldsymbol{V}_{L-1}\}$ the constellation to be designed. By definition of the

Manuscript received August 26, 2006; revised January 16, 2007. This work was supported in part by the Swiss National Science Foundation under Grant PBEL2-110209 and by the National Science Foundation under Grant CCR-0133818, by Caltech's Lee Center for Advanced Networking, and by a grant from the David and Lucille Packard Foundation.

The authors are with the Department of Electrical Engineering, California Institute of Technology, Pasadena, CA 91125 (e-mail: frederique@systems.caltech.edu; hassibi@systems.caltech.edu).

Communicated by I. Dumer, Associate Editor for Coding Theory.

Color versions of Figures 1–3 in this correspondence are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2007.894681

scheme itself, the matrices $\boldsymbol{V}$ have to be unitary (so that the product $\boldsymbol{S}$ does not go to zero or infinity).

Note that since the channel is used M times, the transmission rate is

$$R = \frac{1}{M}\log_2 L. \tag{3}$$

The size $|\mathcal{C}|$ of the constellation is thus $L = 2^{MR}$.

If we further assume the channel constant for $2M$ consecutive uses, we get from (1) and (2) that

$$\begin{aligned}\boldsymbol{Y}_t &= \sqrt{\rho}\boldsymbol{V}_{z_t}\boldsymbol{S}_{t-1}\boldsymbol{H} + \boldsymbol{W}_t \\ &= \boldsymbol{V}_{z_t}(\boldsymbol{Y}_{t-1} - \boldsymbol{W}_{t-1}) + \boldsymbol{W}_t \\ &= \boldsymbol{V}_{z_t}\boldsymbol{Y}_{t-1} + \boldsymbol{W}'_t.\end{aligned}$$

Since the matrix $\boldsymbol{H}$ does not appear in the last equation, this means differential modulation allows decoding without knowledge of the channel.

Note that in practice, the coherence interval is usually much larger than $2M$. In fact, what is often encountered is a continuously fading channel. The assumption that the differential scheme exploits is that the channel is roughly constant over "any" $2M$ channel uses.

The maximum-likelihood (ML) decoder is thus given by

$$\hat{z}_t = \arg\min_{l=0,\ldots,|\mathcal{C}|-1} \|\boldsymbol{Y}_t - \boldsymbol{V}_l\boldsymbol{Y}_{t-1}\|.$$

At high SNR, the pairwise block probability of error P_e can be upper-bounded by [4], [5]

$$P_e \leq \left(\frac{1}{2}\right)\left(\frac{8}{\rho}\right)^{MN} \frac{1}{|\det(\boldsymbol{V}_i - \boldsymbol{V}_j)|^{2N}}.$$

It is thus expected that the bigger $\det(\boldsymbol{V}_i - \boldsymbol{V}_j)$, $i \neq j$ is, the better the code will perform. Thus, the *diversity product*, given by

$$\zeta_{\mathcal{C}} = \frac{1}{2}\min_{\boldsymbol{V}_i \neq \boldsymbol{V}_j} |\det(\boldsymbol{V}_i - \boldsymbol{V}_j)|^{1/M}, \qquad \forall\, \boldsymbol{V}_i \neq \boldsymbol{V}_j \in \mathcal{C} \tag{4}$$

has been defined as a measure of the quality of the code. We say that *full diversity* is achieved when

$$\det(\boldsymbol{V}_i - \boldsymbol{V}_j) \neq 0, \qquad \forall\, \boldsymbol{V}_i \neq \boldsymbol{V}_j \in \mathcal{C}. \tag{5}$$

A design criterion can be summarized as follow: let M be the number of transmit antennas and R be the desired rate. Find a code constellation $\mathcal{C}$ of $L = 2^{MR}$ unitary matrices such that $\zeta_{\mathcal{C}}$ is maximized. Much of the work on differential coding has been on getting fully diverse codes, with the best possible diversity product [8], [16], [7], [6]. However, the Cayley codes approach is different, as recalled in next section.

B. Cayley Differential Codes

Cayley codes for transmission over noncoherent MIMO channels have been introduced in [3]. They are based on the *Cayley transform*, which maps the nonlinear Stiefel manifold to the linear space of Hermitian or skew-Hermitian matrices (and *vice versa*). Let $\boldsymbol{A}$ be a Hermitian matrix, and thus $i\boldsymbol{A}$ be skew-Hermitian. The Cayley transform of $i\boldsymbol{A}$ is given by

$$\boldsymbol{V} = (\boldsymbol{I} + i\boldsymbol{A})^{-1}(\boldsymbol{I} - i\boldsymbol{A}).$$

It is easy to check that $\boldsymbol{V}$ is unitary. The Cayley transform of $i\boldsymbol{A}$ is preferred since all its eigenvalues are strictly imaginary, thus different from 1, so that the inverse of $\boldsymbol{I} + i\boldsymbol{A}$ always exists.

In order to encode information, the Hermitian matrix $\boldsymbol{A}$ is defined by

$$\boldsymbol{A} = \sum_{q=1}^{Q} \alpha_q \boldsymbol{A}_q$$

where $\alpha_1, \ldots, \alpha_Q \in \mathbb{R}$ are the information symbols, chosen from a set $\mathcal{S}$ with r possible values, and where $\boldsymbol{A}_q$ are fixed $M \times M$ complex Hermitian matrices. Let $L = 2^{RM} = r^Q$ be the cardinality of the codebook. The rate of a Cayley code is given by

$$R = \frac{Q}{M}\log_2 r.$$

The reader can refer to [3] for decoding issues.

The performance of a Cayley code depends on Q, the Hermitian basis matrices $\{\boldsymbol{A}_q\}$, and the set $\mathcal{S}$ from which each α_q is chosen. To choose the $\{\boldsymbol{A}_q\}$, the approach of [3] consists in optimizing a mutual information criterion, instead of the traditional diversity criterion (4), since it is argued that at high rate, checking the diversity may become intractable. The $\boldsymbol{A}_1, \ldots, \boldsymbol{A}_Q$ are thus chosen such that the distribution on $\boldsymbol{V}$ is close to the distribution that maximizes the mutual information between it and the pair $(\boldsymbol{Y}_{\tau-1}, \boldsymbol{Y}_\tau)$. It has been shown that the optimal distribution on $\boldsymbol{V}$ is to choose $\boldsymbol{V}$ *isotropically distributed*. (An isotropically distributed unitary matrix $\boldsymbol{V}$ has a probability density function which is invariant to pre- and post-multiplication by an arbitrary unitary matrix.) Consequently, it is shown that the optimal distribution on $\boldsymbol{A}$ is

$$p(\boldsymbol{A}) = \frac{2^{M^2-M}(M-1)!\cdots 1!}{\pi^{M(M+1)/2}} \frac{1}{\det(I + \boldsymbol{A}^2)^M}.$$

The above probability density function is a generalization of the scalar Cauchy distribution, which is why $\boldsymbol{A}$ is said to be *Cauchy distributed*. Finally, using Cauchy matrices is shown to imply that a good choice for the scalars $\alpha_1, \ldots, \alpha_Q$ is to take them scalar-Cauchy distributed. The optimizations are done numerically using a gradient method. The interested reader may consult [3] for the details of the mutual information criterion and the above optimizations.

The drawback of this method is that the mutual information optimization depends on both the number of antennas and the rate, so that heavy computations have to be repeated each time one of these two parameters is changing.

In the following, we are interested in considering similar Cayley codes, except that we will replace the mutual information criterion by the original diversity criterion (4). In order to do so, we need the algebraic concept of *division algebras*, introduced in the next section.

III. Cyclic Algebras

In [3], it has been shown that a set of unitary matrices $\{\boldsymbol{V}_1, \ldots, \boldsymbol{V}_L\}$ is fully diverse (5) if and only if the set of its skew-Hermitian Cayley transform is.

In [15], [11], families of matrices achieving full diversity for the coherent MIMO channel have been found using an algebraic object called *division algebras*, and in particular *cyclic division algebras*. In this section, we recall what these objects are, and how they allow to get families of matrices that are fully diverse (Section III-A). Our aim is then to build sets of Hermitian matrices inside the algebra (Section III-B), which will thus be fully diverse, for building Cayley codes.

For basic algebraic definitions and facts, we let the reader refer for example to [17], [9]. Also, a self-contained tutorial providing the background necessary to understand cyclic-algebra-based codes is available in [1].

A. Basic Definitions

Let L/K be a Galois extension of degree n such that its Galois group $G = \mathrm{Gal}(L/K)$ is cyclic, with generator σ. Choose a nonzero element $\gamma \in K$. We construct a noncommutative algebra, denoted by $\mathcal{A} = (L/K, \sigma, \gamma)$, as follows:

$$\mathcal{A} = L \oplus eL \oplus \cdots \oplus e^{n-1}L$$

such that e satisfies

$$e^n = \gamma \quad \text{and} \quad \lambda e = e\sigma(\lambda), \qquad \text{for } \lambda \in L.$$

Such an algebra is called a *cyclic algebra*. It is a right vector space over L, and as such has dimension $(\mathcal{A} : L) = n$.

Cyclic algebras have been considered for coding applications since they naturally provide families of matrices as follows. Since each $x \in \mathcal{A}$ is expressible as

$$x = x_0 + ex_1 + \cdots + e^{n-1}x_{n-1}, \qquad x_i \in L \text{ for all } i,$$

there is a correspondence between $x \in \mathcal{A}$ and the matrix of left multiplication by x given by

$$\begin{pmatrix} x_0 & \gamma\sigma(x_{n-1}) & \gamma\sigma^2(x_{n-2}) & \cdots & \gamma\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) & \gamma\sigma^2(x_{n-1}) & \cdots & \gamma\sigma^{n-1}(x_2) \\ \vdots & & \vdots & & \vdots \\ x_{n-2} & \sigma(x_{n-3}) & \sigma^2(x_{n-4}) & \cdots & \gamma\sigma^{n-1}(x_{n-1}) \\ x_{n-1} & \sigma(x_{n-2}) & \sigma^2(x_{n-3}) & \cdots & \sigma^{n-1}(x_0) \end{pmatrix}. \quad (6)$$

Example 1: For $n = 2$, we have

$$\mathcal{A} = L \oplus eL$$

such that e satisfies

$$e^2 = \gamma \quad \text{and} \quad \lambda e = e\sigma(\lambda), \qquad \text{for } \lambda \in L.$$

Now, an element $x \in \mathcal{A}$ can be written $x = x_0 + ex_1$. Let us compute the multiplication by x of any element $y \in \mathcal{A}$

$$\begin{aligned} xy &= (x_0 + ex_1)(y_0 + ey_1) \\ &= x_0y_0 + x_0ey_1 + ex_1y_0 + ex_1ey_1 \\ &= x_0y_0 + e\sigma(x_0)y_1 + ex_1y_0 + \gamma\sigma(x_1)y_1 \end{aligned}$$

since $e^2 = \gamma$ and using the noncommutative rule $\lambda e = e\sigma(\lambda)$. In matrix form in the basis $\{1, e\}$, this yields

$$xy = \begin{pmatrix} x_0 & \gamma\sigma(x_1) \\ x_1 & \sigma(x_0) \end{pmatrix} \begin{pmatrix} y_0 \\ y_1 \end{pmatrix}.$$

There is thus a correspondence

$$x = x_0 + ex_1 \in \mathcal{A} \leftrightarrow \begin{pmatrix} x_0 & \gamma\sigma(x_1) \\ x_1 & \sigma(x_0) \end{pmatrix}.$$

Note that in particular

$$e \in \mathcal{A} \leftrightarrow \begin{pmatrix} 0 & \gamma \\ 1 & 0 \end{pmatrix}. \quad (7)$$

Cyclic algebras provide us with a family $\mathcal{C}$ of matrices of the form (6), which is clearly linear (since σ is). Thus

$$\det(\boldsymbol{X}' - \boldsymbol{X}'') = \det(\boldsymbol{X}), \mathbf{0} \neq \boldsymbol{X} \in \mathcal{C}, \qquad \text{for all } \boldsymbol{X}' \neq \boldsymbol{X}'' \in \mathcal{C}$$

so that the diversity (defined in (4)) simplifies to

$$\zeta_{\mathcal{C}} = \frac{1}{2} \min_{\boldsymbol{X} \neq \mathbf{0}} |\det(\boldsymbol{X})|^{1/M}, \qquad \boldsymbol{X} \in \mathcal{C}.$$

If now the cyclic algebra we consider is also a *field*, that is, by definition, that every element in $\mathcal{A}$ is invertible, this guarantees that $\zeta_{\mathcal{C}} > 0$.

Definition 1: We call a noncommutative field a *division algebra*.

In particular, a cyclic algebra which also has a structure of field is called a *cyclic division algebra*. It is thus enough to consider cyclic division algebras to get $\zeta_{\mathcal{C}} > 0$.

Remark 1: Clearly, only the infinite code can be linear. When considering a finite constellation, the code is not linear anymore, and $\boldsymbol{X}' - \boldsymbol{X}'' = \boldsymbol{X}$ with $\boldsymbol{X}$ which may not belong to the codebook anymore. However, $\boldsymbol{X}$ will still be invertible, which guarantees full diversity.

In order to know whether a cyclic algebra is a division algebra, the following criterion is useful.

Proposition 1: [15]: The algebra $\mathcal{A} = (L/K, \sigma, \gamma)$ of degree n is a division algebra if the smallest positive integer t such that γ^t is the norm of some element in L is n.

B. An Involution on the Algebra

With the notations of Section III-A, let $\mathcal{A} = (L/K, \sigma, \gamma)$ be a cyclic division algebra. We now have a linear family $\mathcal{C}$ of fully diverse matrices (as described in (6)) among which we are looking for Hermitian matrices, i.e., $\boldsymbol{X} \in \mathcal{C}$ such that $\boldsymbol{X} = \boldsymbol{X}^\dagger$, where † denotes the transpose conjugate.

In [10], [12], the problem of finding unitary matrices in a cyclic algebra has been studied. It has been shown that taking the transpose conjugate of a matrix $\boldsymbol{X}$ is equivalent to applying an involution α on the corresponding element $x \in \mathcal{A}$. In other words, since the element $x \in \mathcal{A}$ corresponds to the matrix $\boldsymbol{X}$, one translates the operation "transpose conjugate" on $\boldsymbol{X}$ to some equivalent operation (namely an involution) on the element x

$\mathcal{A}$		$\mathcal{M}_n(L)$
x	$\leftrightarrow$	$\boldsymbol{X}$
$\alpha(x)$	$\leftrightarrow$	$\boldsymbol{X}^\dagger$

With this notation, finding a unitary matrix $\boldsymbol{X}$ such that $\boldsymbol{X}\boldsymbol{X}^\dagger = \boldsymbol{I}$, translates into finding an element $x \in \mathcal{A}$ such that $x\alpha(x) = 1$. Since this approach was successful, it is natural to look for Hermitian matrices by considering the equation $x = \alpha(x)$

$\mathcal{A}$		$\mathcal{M}_n(L)$
$x\alpha(x) = 1$	$\leftrightarrow$	$\boldsymbol{X}\boldsymbol{X}^\dagger = \boldsymbol{I}$
$\alpha(x) = x$	$\leftrightarrow$	$\boldsymbol{X}^\dagger = \boldsymbol{X}$

The involution α gives us a convenient way to work in the algebra $\mathcal{A}$, instead of working in $\mathcal{M}_n(L)$ directly. Let us first recall how the involution was defined on $\mathcal{A}$. Let $\alpha_L : L \to L$ denote the complex conjugation, then $\alpha : \mathcal{A} \to \mathcal{A}$ is given by

$$\begin{aligned} \alpha(x_0 + ex_1 + \cdots + e^{n-1}x_{n-1}) &= \alpha_L(x_0) \\ &\quad + e^{-1}\sigma^{-1}(\alpha_L(x_1)) + \cdots + e^{-(n-1)}\sigma^{-(n-1)}(\alpha_L(x_{n-1})). \end{aligned}$$

We refer to [10], [12] for the technical hypothesis, and the proof that α as defined above indeed gives the correspondence $\alpha(x) \leftrightarrow \boldsymbol{X}^\dagger$.

Example 2: Take $n = 3$ (to obtain 3×3 matrices). Let $\zeta_3 = e^{2i\pi/3}$ be a primitive 3rd root of unity, and similarly let $\zeta_7 = e^{2i\pi/7}$ be a primitive 7th root of unity. Set $\theta = \zeta_7 + \zeta_7^{-1}$. We consider the number field

$$L = \mathbb{Q}(\theta, \zeta_3) = \{a + b\theta + c\theta^2 \mid a, b, c \in \mathbb{Q}(\zeta_3)\}$$

with cyclic Galois group $\mathrm{Gal}(L/\mathbb{Q}(\zeta_3)) = \langle\sigma\rangle$, $\sigma : \zeta_7 + \zeta_7^{-1} \mapsto \zeta_7^2 + \zeta_7^{-2}$. We consider the algebra $\mathcal{A} = (L/K, \sigma, \gamma)$, where $\gamma = \zeta_3$.

We now compute $\alpha(x)$ for $x \in \mathcal{A}$, and show that if $x \leftrightarrow \boldsymbol{X}$, then $\alpha(x) \leftrightarrow \boldsymbol{X}^\dagger$.

Let $\tau : \mathbb{Q}(\zeta_3) \to \mathbb{Q}(\zeta_3)$ be defined by $\tau(u + v\zeta_3) = u + v\zeta_3^2$ and $\zeta_3^2 = -\zeta_3 - 1$. This is clearly the complex conjugation. Since θ is totally real, the complex conjugation α_L on L can be written as

$$\begin{aligned} \alpha_L : L &\to L \\ a + b\theta + c\theta^2 &\mapsto \tau(a) + \tau(b)\theta + \tau(c)\theta^2. \end{aligned}$$

By definition, the involution $\alpha : \mathcal{A} \to \mathcal{A}$ is given by

$$\alpha(x_0 + ex_1 + e^2x_2) = \alpha_L(x_0) + e^{-1}\sigma^2(\alpha_L(x_1)) + e^{-2}\sigma(\alpha_L(x_2)).$$

Since $e^3 = \gamma = \zeta_3$, we have that $e^{-1} = e^2\zeta_3^2$ and $e^{-2} = \zeta_3^2 e$. Thus, the involution can be written as

$$\alpha(x_0 + ex_1 + e^2x_2) = \alpha_L(x_0) + e\zeta_3^2\sigma(\alpha_L(x_2)) + e^2\zeta_3^2\sigma^2(\alpha_L(x_1)).$$

The matrix corresponding to x is

$$\boldsymbol{X} = \begin{pmatrix} x_0 & x_1 & x_2 \\ \zeta_3\sigma(x_2) & \sigma(x_0) & \sigma(x_1) \\ \zeta_3\sigma^2(x_1) & \zeta_3\sigma^2(x_2) & \sigma^2(x_0) \end{pmatrix}.$$

Since $\alpha_L\sigma = \sigma\alpha_L$,[1] we can rewrite $\alpha(x)$, recalling that α_L is the complex conjugation that we denote now by $\bar{}$, as

$$\overline{x_0} + e\zeta_3^2\overline{\sigma(x_2)} + e^2\zeta_3^2\overline{\sigma^2(x_1)}.$$

The matrix of $\alpha(x)$ is thus

$$\boldsymbol{X} = \begin{pmatrix} \overline{x_0} & \zeta_3^2\overline{\sigma(x_2)} & \zeta_3^2\overline{\sigma^2(x_1)} \\ \overline{x_1} & \overline{\sigma(x_0)} & \zeta_3^2\overline{\sigma^2(x_2)} \\ \overline{x_2} & \overline{\sigma(x_1)} & \overline{\sigma^2(x_0)} \end{pmatrix}$$

which is clearly $\boldsymbol{X}^\dagger$.

The characterization we will use in this work is thus

$$\boldsymbol{X} = \boldsymbol{X}^\dagger \iff x = \alpha(x). \tag{8}$$

In words, a family $\{\boldsymbol{X}_j \,|\, \boldsymbol{X}_j = \boldsymbol{X}_j^\dagger, j = 1, \ldots, L\}$ of fully diverse matrices is obtained from a family $\{x_j \,|\, x_j = \alpha(x_j), j = 1, \ldots, L\}$ where $\mathcal{A}$ is a cyclic division algebra.

IV. Constructions in Small Dimensions

In this section, we give the constructions of the Cayley codes for two, three, and four antennas, and the simulation results of these codes compared to known constructions. Recall that a codeword $\boldsymbol{V}$ is obtained by applying the Cayley transform on a skew-Hermitian matrix $i\boldsymbol{A}$ where $\boldsymbol{A}$ is given by

$$\boldsymbol{A} = \sum_{q=1}^{Q} \alpha_q \boldsymbol{A}_q.$$

Cyclic division algebras allow us to construct fully diverse matrices $\boldsymbol{A}$. This allows us some freedom for choosing Q and $\{\alpha_j \in \mathcal{S}, j = 1, \ldots, Q\}$.

- The choice of Q: since an arbitrary $M \times M$ Hermitian matrix is parameterized by M^2 real variables, $Q \leq M^2$. Recall that the rate of a Cayley code is given by $R = (Q/M)\log_2(r)$. In order to get high rate, we thus choose $Q = M^2$.
- The choice of $\mathcal{S}$: since $\boldsymbol{A}$ comes from an algebra $\mathcal{A}$ defined over a number field, $\boldsymbol{A}$ is a $\mathbb{Q}$-linear combination of $\boldsymbol{A}_1, \ldots, \boldsymbol{A}_Q$. We thus need $\mathcal{S} \subset \mathbb{Q}$. This is important to be noticed, though it does not bring any restriction since the coefficients $\alpha_q \in \mathbb{R}$ are represented with finite precision, and thus belong to $\mathbb{Q}$.
- The choice of α_q: we take α_q distributed as Cauchy random variables.

Note finally that the codewords are normalized to have Frobenius norm 1, as suggested in [3].

The general procedure we will use for all the code constructions is as follows.

1) Consider a cyclic division algebra.
2) Solve $x = \alpha(x)$.
3) Use the correspondence $x \leftrightarrow \boldsymbol{X}$ to get a Hermitian matrix $\boldsymbol{X}$ which is fully diverse.
4) Decompose $\boldsymbol{X}$ in a basis of Hermitian matrices, all of them being fully diverse. This will give the basis $\{\boldsymbol{A}_1, \ldots, \boldsymbol{A}_Q\}$ to encode the Cayley code.

A. For Two Transmit Antennas

Consider the cyclic algebra $\mathcal{A} = (\mathbb{Q}(i, \sqrt{5})/\mathbb{Q}(i), \sigma, i)$, where $\sigma : \sqrt{5} \mapsto -\sqrt{5}$ and $\mathbb{Q}(i, \sqrt{5}) = \{a + b\sqrt{5} \,|\, a, b \in \mathbb{Q}(i)\}$. It is known that $\mathcal{A}$ is a division algebra [11]. Let $x \in \mathcal{A}$

$$x = x_0 + ex_1, x_0, x_1 \in \mathbb{Q}(i, \sqrt{5}).$$

Using the characterization (8), we have

$$x_0 + ex_1 = \alpha(x_0) + (-i)e\sigma(\alpha(x_1)).$$

By definition of basis, we can identify the coefficients which yields

$$x_0 = \alpha(x_0) = \overline{x_0}$$

implying that $x_0 \in \mathbb{Q}(\sqrt{5}) = \{a + b\sqrt{5} \,|\, a, b \in \mathbb{Q}\}$. Namely

$$x_0 = a_0 + \frac{\sqrt{5}+1}{2}b_0, \quad a_0, b_0 \in \mathbb{Q}$$

using the integral basis $\{1, (1+\sqrt{5})/2\}$ instead of the canonical basis $\{1, \sqrt{5}\}$. Looking at the second coefficient yields

$$x_1 = a_1 + \frac{1+\sqrt{5}}{2}b_1 = -i\left(a_1 + \frac{1-\sqrt{5}}{2}b_1\right)$$

with $a_1, b_1 \in \mathbb{Q}(i)$. Let $\theta = \frac{1+\sqrt{5}}{2}$. It is easy to solve this equation and to see that

$$\begin{aligned} a_1 &= s(1-\theta) - t\theta \\ b_1 &= t(1-\theta) - s\theta \end{aligned}$$

with $s, t \in \mathbb{Q}$. Thus, x can be written

$$x = [a_0 + \theta b_0] + e[(s(1-\theta) - t\theta) + i(t(1-\theta) - s\theta)].$$

Equivalently, using the matrix representation (7) of e with $\gamma = i$, we have

$$\begin{aligned} \boldsymbol{X} = a_0 &\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b_0 \begin{pmatrix} \theta & 0 \\ 0 & 1-\theta \end{pmatrix} \\ &+ s \begin{pmatrix} 0 & 1-\theta-i\theta \\ i\theta + (1-\theta) & 0 \end{pmatrix} \\ &+ t \begin{pmatrix} 0 & -\theta + i(1-\theta) \\ -i(1-\theta) - \theta & 0 \end{pmatrix}. \end{aligned}$$

We thus get a basis of four matrices

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1-\theta-i\theta \\ i\theta + (1-\theta) & 0 \end{pmatrix}, \begin{pmatrix} \theta & 0 \\ 0 & 1-\theta \end{pmatrix}, \begin{pmatrix} 0 & -\theta + i(1-\theta) \\ -i(1-\theta) - \theta & 0 \end{pmatrix} \right\}.$$

[1] That α_L commutes with $\mathrm{Gal}(L/K)$ is a general requirement [10], [12].

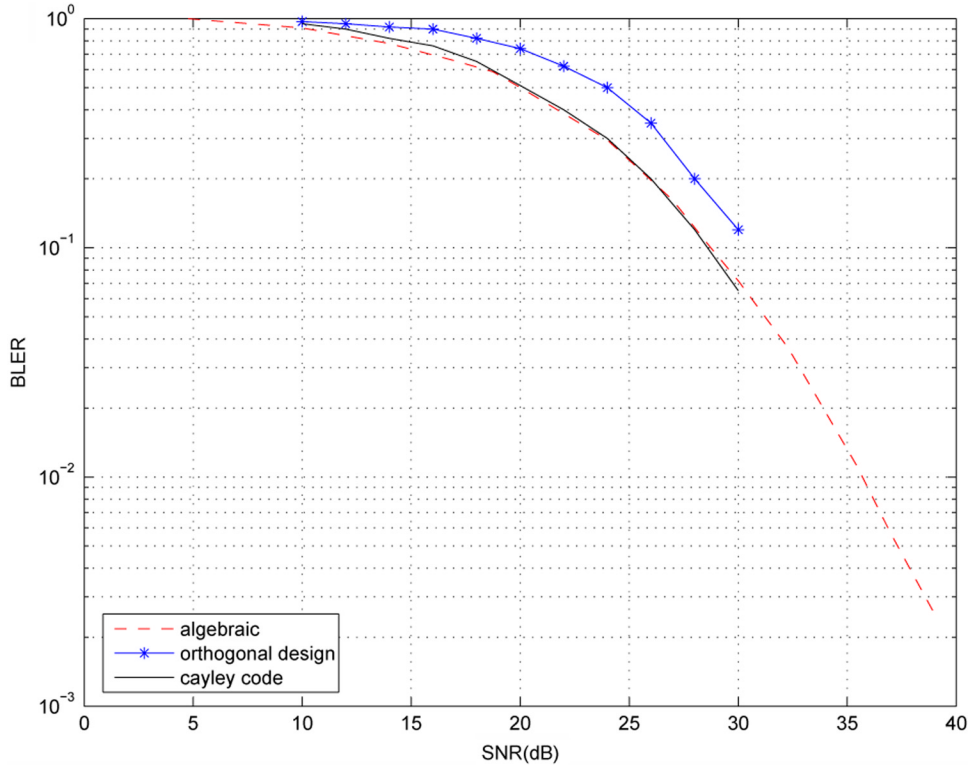

Fig. 1. Performance of unitary codes for $M = 2$ transmit antennas, $N = 2$ receive antennas, and a rate of $R = 6$. The Cayley codes use $Q = 4$ basis matrices. The new Cayley code is simulated at higher SNR.

Each matrix is easily checked to be Hermitian, and after normalizing by the Frobenius norm, we get

$$\left\{ \begin{pmatrix} 0.7071 & 0 \\ 0 & 0.7071 \end{pmatrix}, \begin{pmatrix} 0 & 0.6606 & -0.2523i \\ -0.6606 & -0.2523i & 0 \end{pmatrix}, \right. \\ \left. \begin{pmatrix} 0.9342 & 0 \\ 0 & -0.3568 \end{pmatrix}, \begin{pmatrix} 0 & 0.2523 & -0.6606i \\ -0.2523 & -0.6606i & 0 \end{pmatrix} \right\}.$$

Fig. 1 illustrates the performance of the Cayley code we obtain for $M = 2$ transmit antennas and $N = 2$ receive antennas. The block error rate (BLER) of the new code is given as a function of SNR in decibels. Fig. 1 shows that the algebraic Cayley code is behaving as well as the optimized Cayley code given in [3] for a rate of $R = 6$. It also shows the diversity behavior of the new code (proved to be fully diverse) at higher SNR.

B. For Three Transmit Antennas

Consider the algebra $\mathcal{A} = (\mathbb{Q}(\zeta_3, \zeta_7 + \zeta_7^{-1})/\mathbb{Q}(\zeta_3), \sigma, \zeta_3)$, where $\sigma(\zeta_7 + \zeta_7^{-1}) = \zeta_7^2 + \zeta_7^{-2}$ and $\mathbb{Q}(\zeta_3, \zeta_7 + \zeta_7^{-1}) = \{u + v(\zeta_7 + \zeta_7^{-1}) + w(\zeta_7 + \zeta_7^{-1})^2 \,|\, u, v, w \in \mathbb{Q}(\zeta_3)\} = \{a + b\zeta_3 \,|\, a, b \in \mathbb{Q}(\zeta_7 + \zeta_7^{-1})\}$. It is known that $\mathcal{A}$ is a division algebra [11]. Let $x \in \mathcal{A}$, $x = x_0 + ex_1 + e^2x_2$, with $x_i = a_i + \zeta_3 b_i$, $ai, bi \in \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$, $i = 1, 2, 3$. Note that we choose this representation of x_i to isolate the action of the involution, which only involves ζ_3. The condition $x = \alpha(x)$ gives

$$\begin{cases} x_0 = \alpha(x_0) \\ a_1 = -\sigma(a_2) \\ b_1 = \sigma(b_2) - \sigma(a_2) \end{cases}$$

$a_2, b_2 \in \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$. Set $\theta = \zeta_7 + \zeta_7^{-1}$, $a_2 = s_0 + \theta s_1 + \theta^2 s_2$, and $b_2 = t_0 + \theta t_1 + \theta^2 t_2$. We thus get $x = x_0 + ex_1 + e^2x_2$, with

$$\begin{aligned} x_0 &= u_0 + v_0\theta + w_0\theta^2 \\ x_1 &= -s_0 - s_1(\theta^2 - 2) - s_2(3 - \theta - \theta^2) + \zeta_3[t_1(\theta^2 - 2) \\ &\quad + t_0 + t_2(3 - \theta - \theta^2) - s_0 - s_1(\theta^2 - 2) - s_2(3 - \theta - \theta^2)] \\ x_2 &= s_0 + s_1\theta + s_2\theta^2 + \zeta_3(t_0 + t_1\theta + t_2\theta^2) \end{aligned}$$

with $u_0, v_0, w_0, s_0, s_1, s_2, t_0, t_1, t_2 \in \mathbb{Q}$. In matrix equations, this yields

$$\begin{aligned} \boldsymbol{X} &= u_0 \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} + v_0 \begin{pmatrix} \theta & 0 & 0 \\ 0 & \sigma(\theta) & 0 \\ 0 & 0 & \sigma^2(\theta) \end{pmatrix} \\ &\quad + w_0 \begin{pmatrix} \theta^2 & 0 & 0 \\ 0 & \sigma(\theta^2) & 0 \\ 0 & 0 & \sigma^2(\theta^2) \end{pmatrix} + t_0 \begin{pmatrix} 0 & \zeta_3 & \zeta_3 \\ \zeta_3^2 & 0 & \zeta_3 \\ \zeta_3^2 & \zeta_3^2 & 0 \end{pmatrix} \\ &\quad + s_0 \begin{pmatrix} 0 & -1 - \zeta_3 & 1 \\ \zeta_3 & 0 & -1 - \zeta_3 \\ \zeta_3(-1 - \zeta_3) & \zeta_3 & 0 \end{pmatrix} \\ &\quad + s_1 \begin{pmatrix} 0 & -\theta^2 + 2 - \zeta_3(\theta^2 - 2) & \theta \\ \zeta_3(-2 + \theta^2) & 0 & \zeta_3^2(1 - \theta - \theta^2) \\ \theta & \zeta_3(1 - \theta - \theta^2) & 0 \end{pmatrix} \\ &\quad + s_2 \begin{pmatrix} 0 & \zeta_3^2(3 - \theta - \theta^2) & \theta^2 \\ \zeta_3(3 - \theta - \theta^2) & 0 & \zeta_3^2(2 + \theta) \\ \theta^2 & \zeta_3(2 + \theta) & 0 \end{pmatrix} \\ &\quad + t_1 \begin{pmatrix} 0 & \zeta_3(\theta^2 - 2) & \zeta_3\theta \\ \zeta_3^2(\theta^2 - 2) & 0 & \zeta_3(1 - \theta - \theta^2) \\ \zeta_3^2\theta & \zeta_3^2(1 - \theta - \theta^2) & 0 \end{pmatrix} \\ &\quad + t_2 \begin{pmatrix} 0 & \zeta_3(3 - \theta - \theta^2) & \zeta_3\theta^2 \\ \zeta_3^2(3 - \theta - \theta^2) & 0 & \zeta_3(2 + \theta) \\ \zeta_3^2\theta^2 & \zeta_3^2(2 + \theta) & 0 \end{pmatrix}. \end{aligned}$$

We clearly get a basis of nine Hermitian matrices.

In Fig. 2, we compare the Cayley code with Lie group based codes of [7] by showing their BLER. The performances are close though the Lie group codes are a bit better. This is normal since the Lie codes are optimized for three antennas, which is not the case of the Cayley code. Note that different decoding algorithms are used. Cayley codes

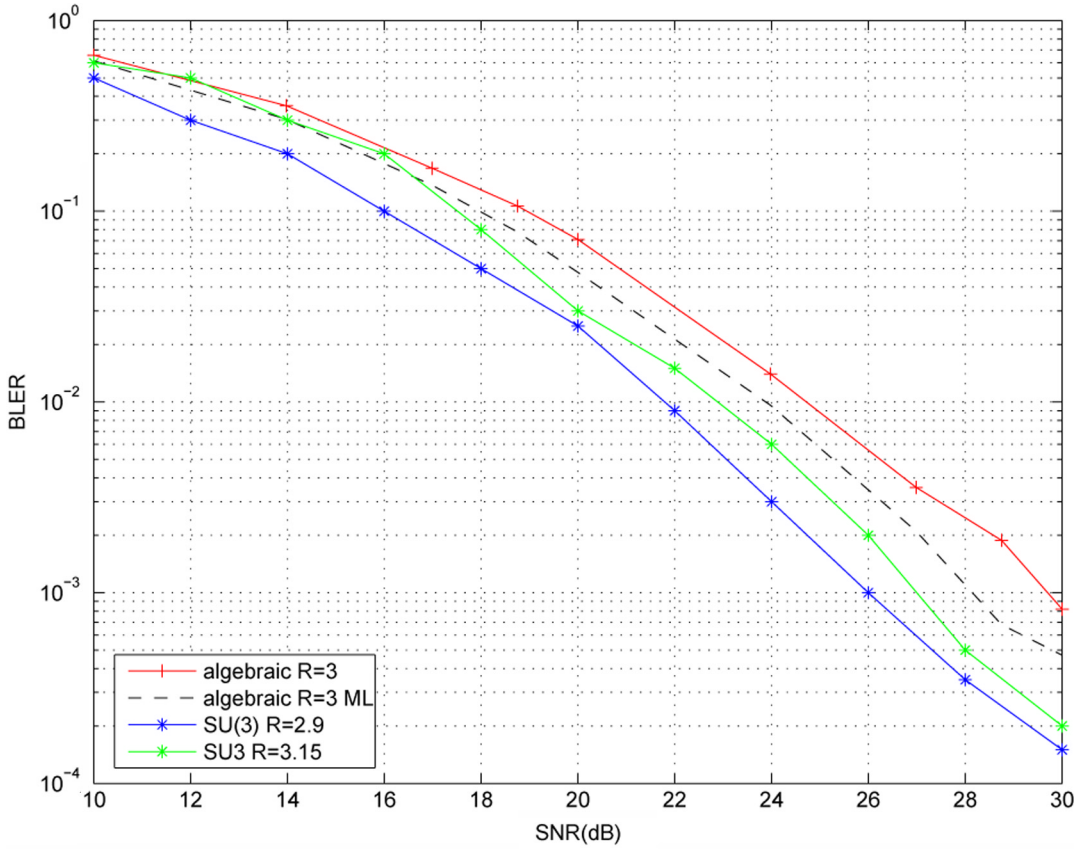

Fig. 2. Performance of unitary codes with $M = 3$ transmit antennas, $N = 1$ receive antenna, and rate $R = 3$. The Cayley code uses $Q = 9$ basis matrices.

are usually not decoded using true ML, but a linearized sphere decoder instead [3]. The performance of the new Cayley code is presented, decoded both by a linearized sphere decoder and a true ML decoder via exhaustive search.

C. For Four Transmit Antennas

We consider the algebra $\mathcal{A} = (\mathbb{Q}(i, \zeta_{15} + \zeta_{15}^{-1})/\mathbb{Q}(i), \sigma, i)$, with $\sigma : \zeta_{15} + \zeta_{15}^{-1} \mapsto \zeta_{15}^{2} + \zeta_{15}^{-2}$ and $\mathbb{Q}(i, \zeta_{15} + \zeta_{15}^{-1}) = \{a + b\theta + c\theta^2 + d\theta^3 \mid a, b, c, d \in \mathbb{Q}(i)\}$, where $\theta = \zeta_{15} + \zeta_{15}^{-1}$. It is known that $\mathcal{A}$ is a division algebra [11]. Let $x = x_0 + ex_1 + e^2x_2 + e^3x_3$ be an element of $\mathcal{A}$. We have

$$x = \alpha(x) \iff \begin{cases} x_0 = \alpha(x_0) \\ x_1 = -i\sigma(\alpha(x_3)) \\ x_2 = -i\sigma^2(\alpha(x_2)) \\ x_3 = -i\sigma^3(\alpha(x_1)). \end{cases}$$

The first equation, as previously, tells that

$$x_0 = a_0 + b_0\theta + c_0\theta^2 + d_0\theta^3, a_0, b_0, c_0, d_0 \in \mathbb{Q}.$$

This yields four diagonal matrices

$$\boldsymbol{X}_0 = a_0 \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} + b_0 \begin{pmatrix} \theta & 0 & 0 & 0 \\ 0 & \sigma(\theta) & 0 & 0 \\ 0 & 0 & \sigma^2(\theta) & 0 \\ 0 & 0 & 0 & \sigma^3(\theta) \end{pmatrix} + c_0 \begin{pmatrix} \theta^2 & 0 & 0 & 0 \\ 0 & \sigma(\theta^2) & 0 & 0 \\ 0 & 0 & \sigma^2(\theta^2) & 0 \\ 0 & 0 & 0 & \sigma^3(\theta^2) \end{pmatrix} + d_0 \begin{pmatrix} \theta^3 & 0 & 0 & 0 \\ 0 & \sigma(\theta^3) & 0 & 0 \\ 0 & 0 & \sigma^2(\theta^3) & 0 \\ 0 & 0 & 0 & \sigma^3(\theta^3) \end{pmatrix}.$$

The third expression only depends on x_2. Writing $x_2 = a_2 + b_2\theta + c_2\theta^2 + d_2\theta^3, a_2, b_2, c_2, d_2 \in \mathbb{Q}(i)$, and solving it gives

$$\begin{cases} a_2 = s_0(i-1) - 5s_1 + s_2 + s_3 \\ b_2 = s_1(1+i) + s_2(-1-4i) + s_3(-4-i) \\ c_2 = (1+i)s_1 \\ d_2 = is_2 + s_3, \end{cases}$$

with $s_0, s_1, s_2, s_3 \in \mathbb{Q}$. The coefficient e^2x_2 can thus be written as the matrix at the top of the following page, with $\lambda_1 = 1-i, \lambda_2 = -1+4i$, and $\lambda_3 = -4+i$. The equations left to solve are

$$\begin{cases} x_1 = -i\sigma(\alpha(x_3)) \\ x_3 = -i\sigma^3(\alpha(x_1)). \end{cases}$$

However, it is easy to see that they are redundant (by applying twice σ on one equation). It suffices thus to consider the first equation. Writing

$$
s_0\begin{pmatrix} 0 & 0 & i-1 & 0 \\ 0 & 1 & 0 & i-1 \\ i(i-1) & 0 & 0 & 0 \\ 0 & i(i-1) & 0 & 0 \end{pmatrix}
+ s_1\begin{pmatrix} 0 & 0 & -5+\bar{\lambda_1}(\theta+\theta^2) & 0 \\ 0 & 0 & 0 & -5+\bar{\lambda_1}(\sigma(\theta)+\sigma(\theta^2)) \\ -5+\lambda_1(\theta+\theta^2) & 0 & 0 & 0 \\ 0 & -5+\lambda_1(\sigma(\theta)+\sigma(\theta^2)) & 0 & 0 \end{pmatrix}
$$

$$
+ s_2\begin{pmatrix} 0 & 0 & 1+\theta\bar{\lambda_2}+i\theta^3 & 0 \\ 0 & 0 & 0 & 1+\sigma(\theta)\bar{\lambda_2}+i\sigma(\theta^3) \\ 1+\theta\lambda_2-i\theta^3 & 0 & 0 & 0 \\ 0 & 1+\sigma(\theta)\lambda_2-i\sigma(\theta^3) & 0 & 0 \end{pmatrix}
+ s_3\begin{pmatrix} 0 & 0 & 1+\theta\bar{\lambda_3}+\theta^3 & 0 \\ 0 & 0 & 0 & 1+\sigma(\theta)\bar{\lambda_3}+\sigma(\theta^3) \\ 1+\theta\lambda_3+\theta^3 & 0 & 0 & 0 \\ 0 & 1+\sigma(\theta)\lambda_3+\sigma(\theta^3) & 0 & 0 \end{pmatrix}
$$

again $x_1 = a_1+b_1\theta+c_1\theta^2+d_1\theta^3, a_1, b_1, c_1, d_1 \in \mathbb{Q}(i)$, and solving the first equation gives

$$
\begin{cases} a_1 = -t_1+2t_3-3t_5+7t_7+i(-t_0+2t_2-3t_4+7t_6) \\ b_1 = 4t_5-3t_7+i(4t_4-3t_6) \\ c_1 = -t_3-3t_7+i(-t_2-3t_6) \\ d_1 = -t_7-t_5+i(-t_4+t_6) \end{cases}
$$

$t_0, \ldots, t_7 \in \mathbb{Q}$. The coefficient $ex_1+e^3x_3$ can thus be written as the matrix at the bottom of the page, with

$$
\lambda_1(\theta) = -7+3\theta+3\theta^2-\theta^3 \quad \text{and} \quad \lambda_2(\theta) = 5+12\theta-3\theta^2-4\theta^3.
$$

We thus get 16 Hermitian matrices. In Fig. 3, we compare, for four transmit antennas and one receive antennas, the new Cayley code to a

$$
t_0\begin{pmatrix} 0 & -i & 0 & 1 \\ i & 0 & -i & 0 \\ 0 & i & 0 & -i \\ 1 & 0 & i & 0 \end{pmatrix} + t_1\begin{pmatrix} 0 & -1 & 0 & i \\ -1 & 0 & -1 & 0 \\ 0 & -1 & 0 & -1 \\ -i & 0 & -1 & 0 \end{pmatrix}
$$

$$
+ t_2\begin{pmatrix} 0 & i(2-\theta^2) & 0 & \theta \\ -i(2-\theta^2) & 0 & -i(1-4\theta+\theta^3) & 0 \\ 0 & i(1-4\theta+\theta^3) & 0 & -i(2+3\theta-\theta^2-\theta^3) \\ \theta & 0 & i(2+3\theta-\theta^2-\theta^3) & 0 \end{pmatrix}
$$

$$
+ t_3\begin{pmatrix} 0 & 2-\theta^2 & 0 & i\theta \\ 2-\theta^2 & 0 & -(1-4\theta+\theta^3) & 0 \\ 0 & -(1-4\theta+\theta^3) & 0 & -(2+3\theta-\theta^2-\theta^3) \\ \theta & 0 & -(2+3\theta-\theta^2-\theta^3) & 0 \end{pmatrix}
$$

$$
+ t_4\begin{pmatrix} 0 & -i(3-4\theta+\theta^3) & 0 & \theta^2 \\ i(3-4\theta+\theta^3) & 0 & -i(4+3\theta-\theta^2-\theta^3) & 0 \\ 0 & i(4+3\theta-\theta^2-\theta^3) & 0 & -i(2+\theta) \\ \theta^2 & 0 & i(2+\theta) & 0 \end{pmatrix}
$$

$$
+ t_5\begin{pmatrix} 0 & -(3-4\theta+\theta^3) & 0 & i\theta^2 \\ -(3-4\theta+\theta^3) & 0 & -(4+3\theta-\theta^2-\theta^3) & 0 \\ 0 & -(4+3\theta-\theta^2-\theta^3) & 0 & -(2+\theta) \\ -i\theta^2 & 0 & -(2+\theta) & 0 \end{pmatrix}
$$

$$
+ t_6\begin{pmatrix} 0 & -i\lambda_1(\theta) & 0 & \theta^3 \\ i\lambda_1(\theta) & 0 & -i(3-15\theta+4\theta^3) & 0 \\ 0 & i(3-15\theta+4\theta^3) & 0 & -i\lambda_2(\theta) \\ \theta^3 & 0 & i\lambda_2(\theta) & 0 \end{pmatrix}
$$

$$
+ t_7\begin{pmatrix} 0 & -\lambda_1(\theta) & 0 & i\theta^3 \\ -\lambda_1(\theta) & 0 & -(3-15\theta+4\theta^3) & 0 \\ 0 & -(3-15\theta+4\theta^3) & 0 & -\lambda_2(\theta) \\ -i\theta^3 & 0 & -\lambda_2(\theta) & 0 \end{pmatrix}
$$

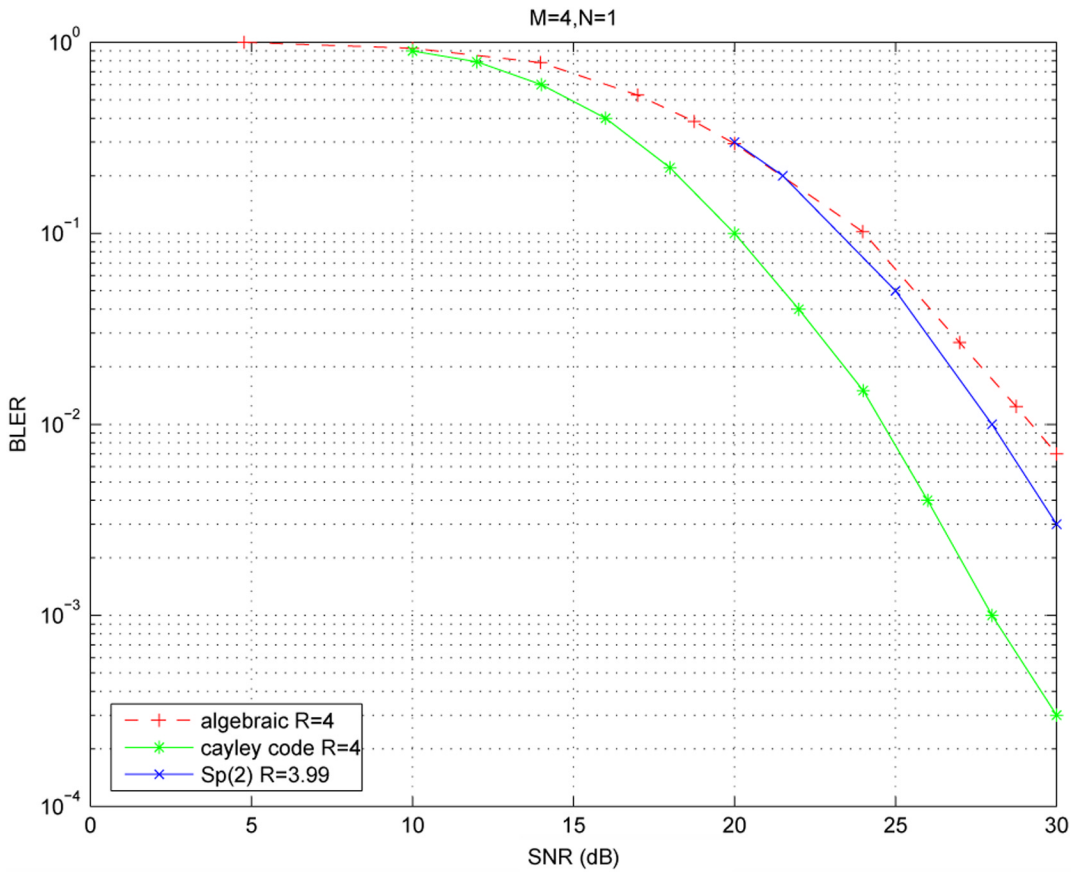

Fig. 3. Performance of unitary codes with $M = 4$ transmit antennas, $N = 1$ receive antenna, and rate $R = 4$. The Cayley codes use $Q = 16$ basis matrices.

Lie group code [6] and to an optimized Cayley code given in [3]. The new Cayley code and the Lie group code are very close. The previous Cayley code clearly performs better. The performance of the previous Cayley code has been reported from [3], where the decoding was done using true ML through exhaustive search. The Lie group has been decoded using a sphere-decoder algorithm, while the new Cayley code has been decoded through a linearized sphere decoder. It was show in Fig. 2 that using a true ML decoder can improve the BLER of the algebraic Cayley code. This is however not significant here, since we are interested in seeing that the new code roughly behaves as well as previously optimized codes.

V. Conclusion

In this work, we looked at Cayley codes for the differential MIMO noncoherent channel. We used division algebras in order to get fully diverse Cayley codes. This yielded a family of codes that naturally fulfills the challenge of performing similarly or closely to previous Cayley codes in dimension $2, 3$, and 4, as well as Lie group based codes in dimension 3 and 4.

References

[1] J.-C. Belfiore, F. Oggier, and E. Viterbo, "Cyclic division algebras: A tool for space-time coding," *Foundations and Trends in Communication and Information Theory*, to be published.

[2] B. Hassibi and H. Vikalo, "On sphere decoding algorithm. I. Expected complexity," *IEEE Trans. Signal Processing*, vol. 53, no. 8, pp. 2806–2818, Aug. 2005.

[3] B. Hassibi and B. Hochwald, "Cayley differential unitary space–time codes," *IEEE Trans. Inf. Theory*, vol. 48, no. 6, pp. 1485–1503, Jun. 2002.

[4] B. Hochwald and W. Sweldens, "Differential unitary space time modulation," *IEEE Trans. Commun.*, vol. 48, no. 12, pp. 2041–2052, Dec. 2000.

[5] B. Hughes, "Differential space–time modulation," *IEEE Trans. Inf. Theory*, vol. 46, no. 7, pp. 2567–2578, Nov. 2000.

[6] Y. Jing and B. Hassibi, "Design of full-diverse multiple-antenna codes based on Sp(2)," *IEEE Trans. Inf. Theory*, vol. 50, no. 11, pp. 2639–2656, Nov. 2004.

[7] ——, "Three-transmit-antenna space-time codes based on SU(3)," *IEEE Trans. Signal Process.*, vol. 53, no. 10, pp. 3688–3702, Oct. 2005.

[8] X.-B. Liang and X.-G. Xia, "Unitary signal constellations for differential space-time modulation with two transmit antennas: Parametric codes, optimal designs, and bounds," *IEEE Trans. Inf. Theory*, vol. 48, no. 8, pp. 2291–2322, Aug. 2002.

[9] F. Oggier and E. Viterbo, "Algebraic number theory and code design for Rayleigh fading channels," *Foundations and Trends in Communications and Information Theory*, vol. 1, pp. 333–415, 2004.

[10] F. Oggier and E. Lequeu, "Families of unitary matrices achieving full diversity," in *Proce. IEEE Int. Symp. Information Theory*, Adelaide, Australia, Sep. 2005, pp. 1173–1177.

[11] F. E. Oggier, G. Rekaya, J.-C. Belfiore, and E. Viterbo, "Perfect space–time block codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 3885–3902, Sep. 2006.

[12] F. Oggier, "Cyclic algebras for noncoherent differential space-time coding," *IEEE Trans. Inf.n Theory*, accepted for publication.

[13] R. S. Pierce, *Associative Algebras*. New York: Springer-Verlag, 1982.

[14] I. Reiner, *Maximal Orders*. New York: Academic, 1975.

[15] B. A. Sethuraman, B. S. Rajan, and V. Shashidhar, "Full-diversity, high-rate space-time block codes from division algebras," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2596–2616, Oct. 2003.

[16] A. Shokrollahi, B. Hassibi, B. M. Hochwald, and W. Sweldens, "Representation theory for high-rate multiple-antenna code design," *IEEE Trans. Inf. Theory*, vol. 47, no. 6, pp. 2335–2367, Sep. 2001.

[17] I. N. Steward and D. O. Tall, *Algebraic Number Theory*. London, U.K.: Chapman and Hall, 1979.
[18] E. Viterbo and J. Boutros, "A universal lattice code decoder for fading channels," *IEEE Trans. Inf. Theory*, vol. 45, no. 5, pp. 1639–1642, Jul. 1999.

Near Orders and Codes

Cícero Carvalho, Carlos Munuera, *Member, IEEE*, Ercilio da Silva, and Fernando Torres

***Abstract*—Høholdt, van Lint, and Pellikaan used order functions to construct codes by means of Linear Algebra and Semigroup Theory only. However, Geometric Goppa codes that can be represented by this method are mainly those based on just one point. In this correspondence, we introduce the concept of near order function with the aim of generalizing this approach in such a way that a wider family of Geometric Goppa codes can be studied on a more elementary setting.**

***Index Terms*—Algebraic geometric Goppa (GG) codes, error-correcting codes, order function, Weierstrass semigroups.**

I. Introduction

Geometric Goppa codes (or GG codes, for short) were constructed by Goppa [6], [7], based on a curve $\mathcal{X}$ over a finite field $\mathbb{F}$, and two $\mathbb{F}$-rational divisors D and G on $\mathcal{X}$. Here, by a *curve* we mean a projective, geometrically irreducible, nonsingular algebraic curve. Usually the divisors D and G are chosen as

- $D = P_1 + \ldots + P_n$;
- $G = \alpha_1 Q_1 + \ldots + \alpha_\ell Q_\ell$,

where the P_is and Q_js are pairwise different $\mathbb{F}$-rational points of $\mathcal{X}$. Then, there are two GG codes associated to the triple $(\mathcal{X}, D, G)$, defined as the images $C_{\mathcal{L}} = C_{\mathcal{L}}(\mathcal{X}, D, G)$ and $C_\Omega = C_\Omega(\mathcal{X}, D, G)$ of the maps

$$ev : f \in \mathcal{L}(G) \mapsto (f(P_1), \ldots, f(P_n)) \in \mathbb{F}^n$$

and

$$\mathrm{res} : \omega \in \Omega(G - D) \mapsto (\mathrm{res}_{P_1}(\omega), \ldots, \mathrm{res}_{P_n}(\omega)) \in \mathbb{F}^n$$

Manuscript received February 2, 2006; revised January 29, 2007. The work of C. Carvalho was supported in part by FAPEMIG, under Grant CEX 605/05; and research done under a joint project of the Millennium Institute for the Global Advancement of Brazilian Mathematics (IM-AGIMB) and Universidade Federal de Uberlândia (UFU). The work of C. Munuera was supported by the "Junta de Castilla y León," España, under Grant VA020-02. The work of E. da Silva was supported in part by FAPEMIG. This correspondence is based on the Ph.D. dissertation of E. da Silva done at IMECC-UNICAMP, SP-Brazil. The work of F. Torres was supported by CNPq-Brazil (306676/03-6) and PRONEX (66. 2408/96-9).

C. Carvalho and E. da Silva are with the Faculdade de Matemática, Universidade Federal de Uberlândia, Uberlândia, 38408-100, Uberlândia, MG-Brazil (e-mail: cicero@ufu.br; ercilio@ufu.br).

C. Munuera is with the Department of Applied Mathematics, University of Valladolid (ETS Arquitectura) 47014 Valladolid, Castilla, Spain (e-mail: cmunuera@arq.uva.es).

F. Torres is with the Universidade Estadual de Campinas, IMECC-UNICAMP, 13083-970, Campinas SP-Brazil (e-mail: ftorres@ime.unicamp.br).

Communicated by G. Zémor, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2007.894663

respectively. According to the residue theorem, these codes are dual to the other, $C_{\mathcal{L}} = C_\Omega^\perp$, hence both constructions provide the same family of codes. Bounds on the dimension and minimum distance of such codes are available from their definition, as they satisfy $k = \ell(G) - \ell(G - D)$, $d \geq n - \deg(G)$ for $C_{\mathcal{L}}$ and $k = i(G - D) - i(G)$, $d \geq \deg(G) - 2\gamma + 2$ for C_Ω, where γ is the genus of $\mathcal{X}$. Soon after its introduction, GG codes became a very important tool in coding theory; for example, Tsfasman, Vladut, and Zink [22] showed that the Varshamov–Gilbert bound can be attained by using these codes. The way of dealing with the dimension and minimum distance of $C_{\mathcal{L}}$ and C_Ω is via the Riemann–Roch theorem; in particular one needs to compute the genus of the underlying curve which may be a difficult task. Thus it will be of interest to construct and manage GG codes by using "elementary methods" only. An important step in this direction was given by Høholdt, van Lint, and Pellikaan [8] (see also [2]), who used order functions (see Section II-B) to construct codes from an $\mathbb{F}$-algebra $\mathbf{R}$. Order functions and the obtained codes have been studied in detail by Pellikaan, Geil, and other authors (see [5], [20]). This technique allows us to do mainly with "one-point GG" codes—that is to say, when $\ell = 1$ in the definition of the divisor G above—. The objective of this correspondence is to introduce and study a wider class of "order-like" functions (the called *near order* functions; see Section III) in such a way that more GG codes could be represented by those elementary methods. In Sections IV and V these near-orders are used to construct codes when $\ell = 2$. The same idea can be applied to obtain codes for general ℓ. However, some subtleties make the case $\ell > 2$ more complicated, and, thus, we do not treat it in this correspondence.

II. Background

A. Weierstrass Semigroups and GG Codes

Let $\mathbb{N}_0$ be the set of nonnegative integers and $\mathbb{F}$ a finite field. For a curve $\mathcal{X}$ over $\mathbb{F}$ and a point $P \in \mathcal{X}$, let $\mathcal{O}_P$ and v_P denote the local ring and valuation of $\mathcal{X}$ at P, respectively. Following [8], we consider the $\mathbb{F}$-algebra

$$\mathbf{R} = \mathbf{R}(Q_1, \ldots, Q_\ell) := \bigcap_{R \neq Q_1, \ldots, Q_\ell} \mathcal{O}_R$$

where the Q_is are as in Section I; we shall consider also the Weierstrass semigroup of $\mathcal{X}$ at $Q_1, \ldots, Q_\ell$, namely $H = H(Q_1, \ldots, Q_\ell) = \{(\beta_1, \ldots, \beta_\ell) \in \mathbb{N}_0^\ell : \text{there exists } f \in \mathbf{R} \text{ with } \mathrm{div}_\infty(f) = \beta_1 Q_1 + \ldots + \beta_\ell Q_\ell\}$.

These semigroups have been intensively studied in connection with coding theory; see for example, [1], [3], [4], [9]–[14], [16]–[19]. The relationship between $\mathbf{R}$ and H above suggests that Goppa codes can be represented by elementary means. As aforementioned, this was noticed in [8] for the case $\ell = 1$ (see also, [15]).

B. Order Functions

Our reference in this section is [8]. Let $\mathbf{R}$ be a commutative $\mathbb{F}$-algebra with identity. In what follows, for short, we refer to $\mathbf{R}$ simply as an $\mathbb{F}$-algebra. A function $\rho : \mathbf{R} \to \mathbb{N}_0 \cup \{-\infty\}$ is called an *order* function if the following properties:

(O0) $\rho(f) = -\infty$ if and only if $f = 0$;
(O1) $\rho(\lambda f) = \rho(f)$ for all $\lambda \in \mathbb{F}^*$;
(O2) $\rho(f + g) \leq \max\{\rho(f), \rho(g)\}$;
(O3) If $\rho(f) < \rho(g)$ and $h \neq 0$, then $\rho(fh) < \rho(gh)$; and
(O4) If $\rho(f) = \rho(g) \neq -\infty$, then there exists $\lambda \in \mathbb{F}^*$ such that $\rho(f - \lambda g) < \rho(g)$;

are satisfied for all $f, g, h \in \mathbf{R}$. If in addition

(O5) $\rho(fg) = \rho(f) + \rho(g)$;